

F05-513  
I.D.S



(19)日本国特許庁 (JP) (12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2000-295274  
(P2000-295274A)

(43)公開日 平成12年10月20日(2000. 10. 20)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマート*(参考)
H 0 4 L 12/56		H 0 4 L 11/20	1 0 2 D 5 K 0 3 0 9 A 0 0 1

審査請求 有 請求項の数7 O L (全 14 頁)

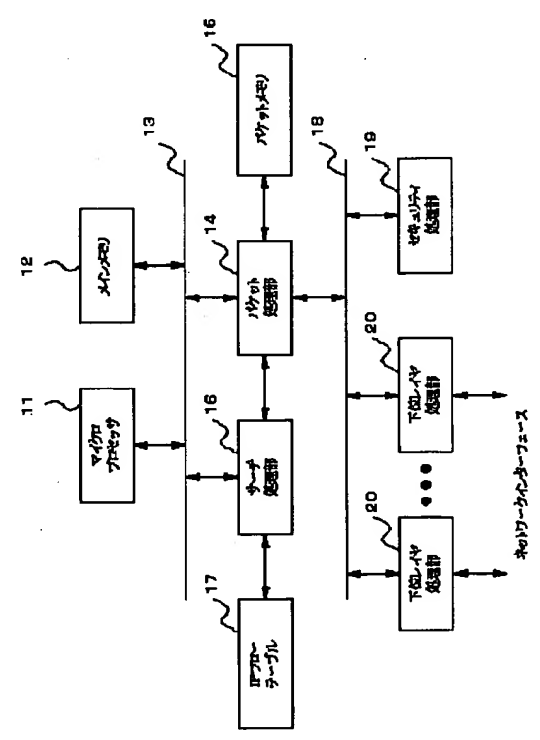
<p>(21)出願番号 特願平11-98140</p> <p>(22)出願日 平成11年4月5日(1999. 4. 5)</p>	<p>(71)出願人 000004237 日本電気株式会社 東京都港区芝五丁目7番1号</p> <p>(72)発明者 亀谷 潤 東京都港区芝五丁目7番1号 日本電気株式会社内</p> <p>(74)代理人 100093595 弁理士 松本 正夫</p> <p>Fターム(参考) 5K030 GA01 HA08 HB11 HD09 KA01 KA13 KA17 LB05 LD19 9A001 BB06 CC03 CC07 EE01 EE03 KK56 LL03</p>
------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(54)【発明の名称】 パケット交換装置

(57)【要約】 (修正有)

【課題】 ルーティング処理及びセキュリティ処理におけるマイクロプロセッサの負担を軽減して、パケット交換処理の高速化を実現する。

【解決手段】 IP発信元アドレスとIP宛先アドレスとをサーチキーとして、ルーティング処理の結果を登録し、保持するIPフローテーブル17と、パケットを受信した場合に、IP発信元アドレス及びIP宛先アドレスをサーチキーとしてIPフローテーブルを検索16し、該当IPフローが登録されていた場合、マイクロプロセッサ11によるルーティング処理へ移行することなく、IPフローに示されるルーティング処理結果に基づいて、適切な出力ポートへ転送するパケット処理実行手段14と、ネットワークインタフェースと接続され、受け取ったパケットに対し下位レイヤの処理を実行し送出する下位レイヤ処理手段20を備える。



## 【特許請求の範囲】

【請求項1】 パケット通信ネットワークに用いられ、パケット単位でルーティング処理を実行しパケット転送を行うパケット交換装置において、ソフトウェア制御により受信パケットのルーティング処理を行うマイクロプロセッサと、前記マイクロプロセッサによりルーティング処理がなされたパケットに関して、IP発信元アドレスとIP宛先アドレスとをサーチキーとして、ルーティング処理の結果を登録し、保持するIPフローテーブルと、パケットを受信した場合に、該受信パケットのIP発信元アドレス及びIP宛先アドレスをサーチキーとして前記IPフローテーブルを検索し、検索の結果、該当するIPフローが登録されていた場合、前記マイクロプロセッサによるルーティング処理へ移行することなく、該IPフローに示されるルーティング処理結果に基づいて、該パケットを適切な出力ポートへ転送するパケット処理実行手段と、ネットワークインタフェースと接続され、受信したパケットに対して下位レイヤの処理を実行して前記パケット手段に転送し、前記パケット手段から受け取ったパケットに対して下位レイヤの処理を実行してネットワークへ送出する下位レイヤ処理手段とを備えることを特徴とするパケット交換装置。

【請求項2】 パケットの暗号化処理及び復号化処理を専用のハードウェアによって行うセキュリティ処理手段をさらに備え、前記マイクロプロセッサが、所定の規則に基づいてパケットを暗号化または復号化すべきと判断した場合に、セキュリティ情報として暗号化または復号化の処理方式及び該処理に要する暗号鍵を決定して、前記セキュリティ処理手段に通知し、前記セキュリティ処理手段が、前記マイクロプロセッサから受け取ったセキュリティ情報に基づいてパケットの暗号化処理または復号化処理を実行することを特徴とする請求項1に記載のパケット交換装置。

【請求項3】 前記IPフローテーブルが、前記ルーティング処理の結果に加えて、前記マイクロプロセッサによって決定された前記セキュリティ情報を登録し、前記パケット処理実行手段が、前記受信パケットのIP発信元アドレス及びIP宛先アドレスをサーチキーとして前記IPフローテーブルを検索した結果、該当するIPフローが登録されておりかつ該IPフローエントリに前記セキュリティ情報が登録されていた場合に、前記マイクロプロセッサによる前記セキュリティ情報の取得処理へ移行することなく、該IPフローに示される前記セキュリティ情報と共に前記受信パケットを前記セキュリティ処理手段に送り、前記セキュリティ処理手段が、前記パケット処理実行手段から受け取ったセキュリティ情報に基づいてパケット

の暗号化処理または復号化処理を実行することを特徴とする請求項2に記載のパケット交換装置。

【請求項4】 前記マイクロプロセッサと前記パケット処理実行手段とがプロセッサバスを介して接続されており、前記パケット処理実行手段と前記下位レイヤ処理手段とが所定のスイッチファブリックを介して接続されており、かつ前記セキュリティ処理手段が前記下位レイヤ処理手段と同一のスイッチファブリックに接続されていることを特徴とする請求項2または請求項3に記載のパケット交換装置。

【請求項5】 前記パケット処理実行手段が、前記セキュリティ処理手段により暗号化処理を施されるパケットを、該パケットを転送先のパケット装置との間で用いられる通信パケットでカプセル化することを特徴とする請求項2または請求項3に記載のパケット交換装置。

【請求項6】 パケット通信ネットワークに用いられ、パケット単位でルーティング処理を実行しパケット転送を行うパケット交換装置において、ソフトウェア制御により受信パケットのルーティング処理を行うマイクロプロセッサと、パケットの暗号化処理及び復号化処理を専用のハードウェアによって行うセキュリティ処理手段と、ネットワークインタフェースと接続され、パケットの送受信を行うと共に、受信したパケット及び送信するパケットに対して下位レイヤの処理を実行する下位レイヤ処理手段とを備え、前記マイクロプロセッサが、所定の規則に基づいてパケットを暗号化または復号化すべきと判断した場合に、セキュリティ情報として暗号化または復号化の処理方式及び該処理に要する暗号鍵を決定して、前記セキュリティ処理手段に通知し、前記セキュリティ処理手段が、前記マイクロプロセッサから受け取ったセキュリティ情報に基づいてパケットの暗号化処理または復号化処理を実行することを特徴とするパケット交換装置。

【請求項7】 前記マイクロプロセッサと前記下位レイヤ処理手段とが所定のスイッチファブリックを介して接続されており、かつ前記セキュリティ処理手段が前記下位レイヤ処理手段と同一のスイッチファブリックに接続されていることを特徴とする請求項6に記載のパケット交換装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、パケット通信ネットワークにおいて用いられるパケット交換装置に関し、特にマイクロプロセッサの負担を軽減してルーティング処理の高速化を図ったパケット交換装置に関する。

## 【0002】

【従来の技術】 インターネットに代表されるパケット通信ネットワークでは、パケット単位でデータの伝送が行

われる。パケットにはデータの発信元や宛先のアドレス等に関する情報を含むヘッダが付されており、ルータ等のパケット交換装置が、当該ヘッダ部分のアドレス情報に基づき、パケット単位で適切なネットワークへと転送する。

【0003】従来、パケットのルーティング処理は、パケット単位でのルーティング処理という仕組みのため、ソフトウェアで実装されることが多かった。パケットのルーティング処理を実行する従来のパケット交換装置の構成を図9に示す。図9に示すパケット交換装置は、データリンク層以下の処理をハードウェアで実行する下位レイヤ処理部110と、マイクロプロセッサ101、マイクロプロセッサ101上のソフトウェアやルーティング情報を格納するためのメインメモリ102、受信したパケットを格納しておくパケットメモリ105、および下位レイヤ処理部110とパケットメモリ105の間でパケットデータを転送するためのDMAコントローラ112を備える。

【0004】図9に示すように構成された従来のルータにおいてパケットを受信すると、DMAコントローラ112が、一旦、受信した当該パケットを下位レイヤ処理部110からパケットメモリ105に転送しておく。この後、マイクロプロセッサ101が、プロセッサバス103を経由してパケットメモリ105上のパケットをメインメモリ102にコピーする。そして、ソフトウェア制御によりルーティング処理を行い、当該処理によってMACヘッダを付替えたパケットを、再びパケットメモリ105にコピーする。次に、DMAコントローラ112が、当該処理済パケットを出力物理ポートに接続する下位レイヤ処理部110へと転送し、下位レイヤ処理部110による処理の後にネットワークへと送信される。

【0005】以上のように、従来のパケット交換装置は、全ての受信パケットに対するルーティング処理を、ソフトウェア制御によりマイクロプロセッサ101が行うため、ネットワーク速度はマイクロプロセッサ101自身の性能に依存していた。

【0006】ところで、パケット通信方式は、回線交換方式に比べデータのセキュリティが弱いことが従来から指摘されている。また、近年のインターネットの急激な普及により、パケット通信におけるセキュリティ対策が急務となった。そこで、ネットワークレイヤでのセキュリティ対策として、IPパケットデータを暗号化する方式(IPsec)が標準化された。従来のパケット交換装置においては、当該IPsecによるパケットデータの暗号化/復号化処理もマイクロプロセッサ101が全て行っていた。

【0007】

【発明が解決しようとする課題】上述したように、従来のパケット交換装置は、全ての受信パケットに対するルーティング処理を、ソフトウェア制御によりマイクロ

ロセッサが行っていたため、ネットワーク速度はマイクロプロセッサ自身の性能に依存していた。したがって、通信トラヒックの増加やネットワーク速度の高速化の要請に対して、マイクロプロセッサの性能による限界があるという欠点があった。

【0008】図9に示したパケット交換装置において、パケットメモリ105とメインメモリ102とを同一のメモリ素子にて構成することにより、メモリ間のデータ転送に要する時間を短縮することが可能である。しかし、依然としてパケット毎の処理は全てマイクロプロセッサの負荷となるため、処理の高速化に対してマイクロプロセッサの性能による限界があるという欠点は解決されない。

【0009】また、パケット通信におけるセキュリティを向上させるため、従来のパケット交換装置に、上述したIPsecによるパケットデータの暗号化/復号化処理を実装する場合、当該処理を実行するためにマイクロプロセッサの能力を割かれるため、パケット交換装置における全体的な処理性能が低下し、処理の高速化に対する限界をさらに引き下げるという欠点があった。

【0010】具体的には、上記従来のパケット交換装置に、IPsec処理を新たに追加した場合、パケットのデータスループットが約10分の1にまで低下する場合があった。

【0011】本発明は、上記従来の欠点を解決し、ルーティング処理及びセキュリティ処理におけるマイクロプロセッサの負担を軽減することにより、パケット交換処理の高速化を実現するパケット交換装置を提供することにある。

【0012】

【課題を解決するための手段】上記の目的を達成する本発明は、パケット通信ネットワークに用いられ、パケット単位でルーティング処理を実行しパケット転送を行うパケット交換装置において、ソフトウェア制御により受信パケットのルーティング処理を行うマイクロプロセッサと、前記マイクロプロセッサによりルーティング処理がなされたパケットに関して、IP発信元アドレスとIP宛先アドレスとをサーチキーとして、ルーティング処理の結果を登録し、保持するIPフローテーブルと、パケットを受信した場合に、該受信パケットのIP発信元アドレス及びIP宛先アドレスをサーチキーとして前記IPフローテーブルを検索し、検索の結果、該当するIPフローが登録されていた場合、前記マイクロプロセッサによるルーティング処理へ移行することなく、該IPフローに示されるルーティング処理結果に基づいて、該パケットを適切な出力ポートへ転送するパケット処理実行手段と、ネットワークインタフェースと接続され、受信したパケットに対して下位レイヤの処理を実行して前記パケット手段に転送し、前記パケット手段から受け取ったパケットに対して下位レイヤの処理を実行してネッ

トワークへ送出する下位レイヤ処理手段とを備えることを特徴とする。

【0013】請求項2に記載の本発明の packets 交換装置は、パケットの暗号化処理及び復号化処理を専用のハードウェアによって行うセキュリティ処理手段をさらに備え、前記マイクロプロセッサが、所定の規則に基づいてパケットを暗号化または復号化すべきと判断した場合に、セキュリティ情報として暗号化または復号化の処理方式及び該処理に要する暗号鍵を決定して、前記セキュリティ処理手段に通知し、前記セキュリティ処理手段が、前記マイクロプロセッサから受け取ったセキュリティ情報に基づいてパケットの暗号化処理または復号化処理を実行することを特徴とする。

【0014】請求項3に記載の本発明の packets 交換装置は、前記 IP フローテーブルが、前記ルーティング処理の結果に加えて、前記マイクロプロセッサによって決定された前記セキュリティ情報を登録し、前記パケット処理実行手段が、前記受信パケットの IP 発信元アドレス及び IP 宛先アドレスをサーチキーとして前記 IP フローテーブルを検索した結果、該当する IP フローが登録されておりかつ該 IP フローエントリに前記セキュリティ情報が登録されていた場合に、前記マイクロプロセッサによる前記セキュリティ情報の取得処理へ移行することなく、該 IP フローに示される前記セキュリティ情報と共に前記受信パケットを前記セキュリティ処理手段に送り、前記セキュリティ処理手段が、前記パケット処理実行手段から受け取ったセキュリティ情報に基づいてパケットの暗号化処理または復号化処理を実行することを特徴とする。

【0015】請求項4に記載の本発明の packets 交換装置は、前記マイクロプロセッサと前記パケット処理実行手段とがプロセッサバスを介して接続されており、前記パケット処理実行手段と前記下位レイヤ処理手段とが所定のスイッチファブリックを介して接続されており、かつ前記セキュリティ処理手段が前記下位レイヤ処理手段と同一のスイッチファブリックに接続されていることを特徴とする。

【0016】請求項5に記載の本発明の packets 交換装置は、前記パケット処理実行手段が、前記セキュリティ処理手段により暗号化処理を施されるパケットを、該パケットを転送先のパケット装置との間で用いられる通信パケットでカプセル化することを特徴とする。

【0017】請求項6に記載の本発明の packets 交換装置は、パケット通信ネットワークに用いられ、パケット単位でルーティング処理を実行しパケット転送を行う packets 交換装置において、ソフトウェア制御により受信パケットのルーティング処理を行うマイクロプロセッサと、パケットの暗号化処理及び復号化処理を専用のハードウェアによって行うセキュリティ処理手段と、ネットワークインタフェースと接続され、パケットの送受信を

行うと共に、受信したパケット及び送信するパケットに対して下位レイヤの処理を実行する下位レイヤ処理手段とを備え、前記マイクロプロセッサが、所定の規則に基づいてパケットを暗号化または復号化すべきと判断した場合に、セキュリティ情報として暗号化または復号化の処理方式及び該処理に要する暗号鍵を決定して、前記セキュリティ処理手段に通知し、前記セキュリティ処理手段が、前記マイクロプロセッサから受け取ったセキュリティ情報に基づいてパケットの暗号化処理または復号化処理を実行することを特徴とする。

【0018】請求項7に記載の本発明の packets 交換装置は、前記マイクロプロセッサと前記下位レイヤ処理手段とが所定のスイッチファブリックを介して接続されており、かつ前記セキュリティ処理手段が前記下位レイヤ処理手段と同一のスイッチファブリックに接続されていることを特徴とする。

【0019】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0020】図1は、本発明の一実施形態による packets 交換装置の構成を示すブロック図である。図1を参照すると、本実施形態の packets 交換装置は、マイクロプロセッサ11と、メインメモリ12と、マイクロプロセッサ11とメインメモリ12やその他の周辺処理部とを接続するためのプロセッサバス13と、マイクロプロセッサ11に代わってパケット処理を実行するためのパケット処理部14、パケットメモリ15、サーチ処理部16及び IP フローテーブル17と、パケットの暗号化／符号化処理を行うセキュリティ処理部19と、下位レイヤ処理部20と、パケット処理部14とセキュリティ処理部19と下位レイヤ処理部20とを相互に接続するためのスイッチファブリック18とを備える。なお、図1には、本発明における特徴的な構成のみを記載し、他の一般的な構成については記載を省略してある。

【0021】上記構成において、マイクロプロセッサ11は、ソフトウェア制御により packets 交換装置全体の制御を行うと共に、受信パケットの転送先を決めるルーティング処理や、必要に応じてパケットデータに対する暗号化または復号化の必要性を判断する処理を行う。

【0022】メインメモリ12は、マイクロプロセッサ11を制御するソフトウェアや、所定の処理を行う際に当該処理に関わる各種データを格納する。

【0023】パケット処理部14は、ネットワークインタフェースから受信したパケットに対して、IP ヘッダ処理や出力先ネットワークインタフェースへの転送処理を行う。ここで、IP ヘッダ処理とは、パケットに付加されているヘッダから IP 宛先アドレスや IP 発信元アドレスを抽出する処理、マイクロプロセッサ11によるルーティング処理によって決定された MAC アドレスに応じて新しい MAC ヘッダを生成する処理等を含む。

## 7

【0024】また、パケット処理部14は、パケットヘッダから抽出したサーチキーによりサーチ処理部16を制御してIPフローテーブル17を検索させたり、IPフローテーブル17に新しいIPフローを仮登録させたりする。また、サーチ処理部16によるIPフローテーブル17の検索結果に応じて、取得した出力物理ポートやMACアドレスに基づき、該当パケットのIPヘッダ処理を行う。

【0025】パケットメモリ15は、マイクロプロセッサ11やパケット処理部14による処理のために受信パケットを一時的に格納する。また、マイクロプロセッサ11がルーティング処理を行う際に処理結果を待つパケットを登録するプロセッサ処理結果待ちキューを有する。

【0026】サーチ処理部16は、パケット処理部14からの指示にしたがって、IPフローテーブル17を検索し、登録されている該当パケットに関するルーティング処理の結果をパケット処理部14に返す。また、パケット処理部14からの指示に対応するIPフローエントリが存在しない場合、当該指示に基づいてIPフローの仮登録を行う。さらに、マイクロプロセッサ11によるルーティング処理の結果を受け取って、仮登録のIPフローエントリに格納し、当該IPフローを正式登録する。

【0027】IPフローテーブル17は、IP発信元アドレスとIP宛先アドレスとをサーチキーとして、マイクロプロセッサ11によるルーティング処理の結果であるIPフローを格納したテーブルである。図2にIPフローテーブル17の例を示す。図2を参照すると、IPフローテーブル17には、IPフローエントリごとに、サーチキーであるIP発信元アドレス及びIP宛先アドレスと、ルーティング処理の結果であるMAC発信元アドレス、MAC宛先アドレス及び出力物理ポートのポート番号とが登録されている。また、必要に応じて、後述するセキュリティ情報が格納されている。

【0028】スイッチファブリック18は、複数のネットワークインタフェースと個別に接続された複数の下位レイヤ処理部20と、パケット処理部14と、セキュリティ処理部19とを相互に接続する。スイッチファブリック18としては、接続された各ユニット間のデータ転送時の調停機能やアドレッシング機能を持っていれば何でも良く、単純なTri-stateバス、リングバス、クロスバススイッチなど実現手段は問わない。また、スイッチファブリック18の構成をトークンリングバス構成としても良い。

【0029】セキュリティ処理部19は、マイクロプロセッサ11によるソフトウェア処理に基づき、必要に応じて、パケット毎に暗号化/復号化処理を実行する。

【0030】下位レイヤ処理部20は、物理的なネットワークインタフェースと接続され、データリンク層（O

## 8

SI7レイヤモデルの第2層）以下の処理を実行し、スイッチファブリック18を介してパケット処理部14との間でパケットの送受信を行う。

【0031】以上、本実施形態の構成を説明したが、実際には、本実施形態のパケット交換装置は上記各構成要素の機能を実現する各種の回路にて構成され、例えば、上記各構成要素を内包する半導体集積回路にて構成しても良い。

【0032】次に、図3乃至図7のフローチャートを参照して本実施形態の動作について説明する。図3は、本実施形態によるパケット処理の主要な流れを示すフローチャートである。図4は、マイクロプロセッサ11によるルーティング処理の流れを示すフローチャートである。図5乃至図7は、セキュリティ処理を伴う場合の本実施形態によるパケット処理の流れを示すフローチャートである。

【0033】本実施形態のパケット交換装置は、インターネットに代表されるパケット通信のネットワークレイヤの処理を行う装置であるため、ネットワークインタフェースより受信したパケットのヘッダを解析し、その宛先アドレス（IP宛先アドレス）に基づくルーティング処理を行い、その結果にしたがって出力先のネットワークインタフェースへパケットを転送する動作が基本となる。加えて、本実施形態では、受信パケットのルーティング処理の際にIP宛先アドレスとIP発信元アドレスに基づき、必要に応じて、パケット単位にデータの暗号化/復号化等のセキュリティ処理を併せて実行する。したがって、以下の動作の説明では、先に通常のセキュリティ処理を実施しない場合の動作について説明し、次にセキュリティ処理を実行する場合の動作を説明する。

【0034】図3を参照すると、まず、パケット交換装置の外部のネットワークと接続された下位レイヤ処理部20に外部装置からパケットが到着すると（ステップ301）、当該下位レイヤ処理部20は、レイヤ2以下のパケット処理、すなわちデータの同期確立、下位レイヤヘッダ（MACヘッダ等）の検証、CRCの検算等を実行する（ステップ302）。そして、下位レイヤの処理を終えたパケットを、スイッチファブリック18を経由してパケット処理部14へと転送する。

【0035】パケット処理部14は、転送された受信パケットを受け取ると、まず当該パケットをパケットメモリ15に格納する。そして、当該パケットのパケットヘッダからIP宛先アドレスやIP発信元アドレス等を抽出し、これらからIPフローテーブル17を検索するためのサーチキーを作成する（ステップ303）。次に、パケット処理部14は、作成したサーチキーをサーチ処理部16へ送り、IPフローテーブル17の検索を指示する。

【0036】サーチ処理部16は、パケット処理部14から受け取ったサーチキーを用いてIPフローテーブル

17の検索を行い、その結果をパケット処理部14に通知する(ステップ304)。サーチ処理部16による検索の結果、IPフローテーブル17に受信したパケットに相当するIPフローが登録されている場合、すなわち、マイクロプロセッサ11により当該IPフローに対応するパケットに対するルーティング処理が既に行われていた場合は、パケット処理部14は、サーチ処理部16から検索結果(図2に示すIPフローテーブル17ではMAC発信元アドレス、MAC宛先アドレス及び出力物理ポートのポート番号)を受け取り、当該情報に基づいて当該パケットのヘッダ処理を行う(ステップ305、306)。そして、当該情報が示す出力物理ポートに接続された下位レイヤ処理部20へ当該パケットを転送する(ステップ307)。以上の動作により、当該パケットに関しては、ソフトウェア制御によるマイクロプロセッサ11のルーティング処理を行うことなく、パケット処理部14が自律的にパケットの転送を実行することができる。

【0037】下位レイヤ処理部20は、スイッチファブリック18を介してパケット処理部14からパケットを受け取り、下位レイヤ固有の処理、すなわちパケット全体のCRC演算、及び当該演算結果をパケットに付加する処理を行って(ステップ308)、自身が接続されているネットワークインタフェースへ当該パケットを送出する(ステップ309)。

【0038】これに対し、サーチ処理部16による検索の結果、IPフローテーブル17に受信したパケットに相当するIPフローが登録されていない場合、パケット処理部14は、サーチ処理部16に指示してIP宛先アドレス及びIP発信元アドレスをサーチキーとする新しいIPフローの仮登録を実行させる(ステップ305、310)。これは、図2のIPフローテーブルにおいて、サーチキーの項だけが存在するエントリに相当する。次に、パケット処理部14は、マイクロプロセッサ11に対して割り込みを掛けて、マイクロプロセッサ11によるルーティング処理へ当該パケットを引き渡す(ステップ311)。そして、当該パケットをパケットメモリ15のプロセッサ処理結果待ちのキューに登録した後、パケット処理部14は、次のパケットの処理へと移行する(ステップ312)。

【0039】この後、パケット処理部14は、新たに受信したパケット処理の合間に、パケットメモリ15のプロセッサ処理結果待ちキューのパケットを調べ、キューの先頭に置かれたパケットのサーチキーを作成し、サーチ処理部16を制御してIPフローテーブル17の検索を実行する(ステップ313)。後述するように、当該パケットに対するマイクロプロセッサ11によるルーティング処理が完了したならば、該当するIPフローエントリは正式登録されており、検索結果としてMAC発信元アドレス、MAC宛先アドレス及び出力物理ポートの

ポート番号が得られる(ステップ314)。そして、パケット処理部14は、得られたMACアドレス及び出力物理ポートのポート番号に基づいて当該パケットのヘッダ処理を行う(ステップ315)。以下、パケットを下位レイヤ処理部20へ転送し、下位レイヤ固有の処理の後、ネットワークインタフェースへ送出する(ステップ307、308、309)。

【0040】この後、同一のIP発信元アドレス及びIP宛先アドレスを有するパケットを受信した場合は、対応するIPフローがIPフローテーブル17に登録されているため、ステップ305、306及び307の処理により、当該パケットに関して、ソフトウェア制御によるマイクロプロセッサ11のルーティング処理を行うことなく、パケット処理部14が自律的にパケットの転送を実行できることとなる。

【0041】次に、ステップ311により、マイクロプロセッサ11によるルーティング処理へ当該パケットが引き渡された場合のマイクロプロセッサ11の動作を説明する。図4を参照すると、マイクロプロセッサ11は、パケット処理部14からの割り込みに応じてルーティング処理を開始し、まず、プロセッサバス13及びパケット処理部14を介してパケットメモリ15にアクセスする(ステップ401)。そして、パケットメモリ15のプロセッサ結果処理待ちキューから、登録されているパケットのヘッダ部分のみを、メインメモリ12へコピーする(ステップ402)。

【0042】次に、マイクロプロセッサ11は、コピーされたパケットヘッダ部のIP宛先アドレスをキーとして、メインメモリ12に予め格納されているIPルーティングテーブル及びARPキャッシュテーブルの検索を実行する(ステップ403)。そして、パケットの転送先となる出力物理ポート及びネクストホップのMACアドレスを決定する(ステップ404)。そして、これら一連のルーティング処理結果を、プロセッサバス13及びサーチ処理部16を介してIPフローテーブル17に送り、仮登録済みのIPフローエントリの正式登録を行う(ステップ405)。この動作は、図2に示すIPフローテーブル17の該当エントリに、ルーティング結果が追記されたことに相当する。

【0043】次に、パケット単位のセキュリティ処理を伴う場合の本実施形態の動作について説明する。セキュリティ処理として、IETF(Internet Engineering Task Force)で定められたIPsecに対する処理を行う場合を例として説明する。

【0044】IPsecをルータ等のパケット交換装置に実装する場合、パケットを転送したい相手先ホストが所属するネットワークに存在するパケット交換装置との間で、パケットの暗号化方式や暗号鍵の情報を予め共有し、そのパケットを当該パケット交換装置間どうしの通

10

20

30

40

50

信パケットでカプセル化する方法（トンネルモード）を使用する。パケットの暗号化方式と暗号鍵の共有は通信するホスト間で一意であり、したがってパケット交換装置は、IP宛先アドレスとIP発信元アドレスから、当該パケットに適用すべき暗号化方式と暗号鍵を決定できる。これらの共有情報は当該パケット交換装置どうしの間で事前に、または必要に応じて確立する必要がある。本実施形態では、共有情報の確立に付随する処理は全て、ソフトウェア制御によりマイクロプロセッサ11が処理する。IPsecトンネルモードによって処理されたIPパケットの構成を図8に示す。

【0045】本動作例において、パケット交換装置にパケットが到着してからIPフローがIPフローテーブル17に仮登録され、マイクロプロセッサ11によるルーティング処理へパケットが引き渡されるまでの処理は、図3に示した通常の動作と同様である（ステップ301～305、310、311参照）。

【0046】図5を参照すると、マイクロプロセッサ11は、パケット処理部14からの割り込みに応じてルーティング処理を開始し、まず、プロセッサバス13及びパケット処理部14を介してパケットメモリ15にアクセスする（ステップ501）。そして、パケットメモリ15のプロセッサ結果処理待ちキューから、登録されているパケットのヘッダ部分のみを、メインメモリ12へコピーする（ステップ502）。

【0047】次に、マイクロプロセッサ11は、コピーされたパケットヘッダ部のIP宛先アドレスを識別する（ステップ503）。当該パケットが図8に示したようなIPsecヘッダを持つパケットであり、かつ当該IPアドレスが自装置（パケット交換装置）のIPアドレスであるならば、IPsecの復号化対象パケットとして認識する（ステップ504）。また、IPアドレスが自装置のIPアドレスでないならば、IPsecの暗号化対象パケットとして認識する（ステップ505）。

【0048】まず、図6を参照して、IPsec暗号化対象パケットに対する処理について説明する。この場合、マイクロプロセッサ11は、パケットヘッダ部のIP宛先アドレスをキーとして、メインメモリ12に予め格納されているセキュリティ処理に関するテーブル（Security Policy DatabaseとSecurity Association Database）を検索して、当該パケットを暗号化する必要があるかを判断する（ステップ601）。暗号化する必要があると判断された場合、これ以降の動作は図4に示した通常のルーティング処理と同一であり、ルーティングテーブル、ARPキャッシュテーブルの検索、検索結果のIPフローテーブル17への登録を実行する（ステップ403～405参照）。

【0049】パケットを暗号化する場合、マイクロプロセッサ11は、セキュリティ処理のテーブル

検索により得られた暗号化方式及び暗号鍵を含むセキュリティ情報、セキュリティ情報を識別するインデックス（SPI）等と、カプセル化するIPパケットのIP宛先アドレスおよびIP発信元アドレスとを、セキュリティ処理部19が接続された物理ポートを指すルーティング情報と共に、サーチ処理部16を介してIPフローテーブル17に送り、仮登録済みのIPフローエントリの正式登録を行う（ステップ602）。この動作は、図2に示すIPフローテーブル17の該当IPフローエントリに、出力物理ポートと、セキュリティ情報を登録することに相当する。

【0050】パケット処理部14は、当該IPフローに属するパケットに関してサーチ処理部16によるIPフローテーブル17の検索を行った際に、暗号化方式が指定されていることからIPsec暗号化対象パケットであると判断する。そして、当該パケットをIPフローテーブル17に指定されたIP宛先アドレスとIP発信元アドレスのパケットでカプセル化し、暗号化方式等のセキュリティ情報を当該カプセル化されたパケットに付加した後、指定された転送先であるセキュリティ処理部19へ転送する（ステップ603）。

【0051】セキュリティ処理部19は、受け取ったパケットからセキュリティ情報を分離し、得られたセキュリティ情報に従って当該パケットをIPsec暗号化処理した後、再びパケット処理部14へ転送する（ステップ604）。

【0052】パケット処理部14は、セキュリティ処理部19から受け取ったパケットを、外部のネットワークインタフェースから入力されたパケットと特に区別せず、通常のパケットの様に扱ってIPフローテーブル17の検索を実行する（ステップ605）。この際、パケットは既に新しいIP宛先アドレスとIP発信元アドレスでカプセル化されているため、パケット処理部14は、新しいIPフローとしてIPフローテーブル17へ仮登録する。

【0053】この後、マイクロプロセッサ11がルーティング処理を行い、処理結果をIPフローテーブル17へ送ってIPフローエントリの正式登録を行う（ステップ606）。当該パケットに関しては、セキュリティ処理が既に行われていることが判定可能であるため、セキュリティ処理を再実行することはない。

【0054】以上の処理を経た暗号化処理済みのパケットは、これ以降、通常のパケット同様に処理される（図3、ステップ313～315、ステップ307～309参照）。また、これ以降、当該暗号化対象のパケットと同一のサーチキー（IP発信元アドレス及びIP宛先アドレス）を有するパケットを受信した場合は、対応するIPフローがIPフローテーブル17に登録されているため、当該登録されているセキュリティ情報を用いて暗号化処理を行うことが可能である。したがって、通常の



パケットに対するルーティング処理の省略と同様に、マイクロプロセッサ11がセキュリティ情報を取得する処理を行うことなく、パケットがパケット処理部14からセキュリティ処理部19へ送られ、自律的に暗号化処理を実行できることとなる。

【0055】次に、図7を参照して、IPsec復号化対象パケットに対する処理について説明する。この場合、マイクロプロセッサ11は、当該パケットのIPsecヘッダからSPIを抽出し、これをキーとしてメインメモリ12のセキュリティ処理のテーブル(Security Association Database)を検索し、該当する暗号化方式、暗号鍵を得る(ステップ701)。次に、マイクロプロセッサ11は、取得した暗号化方式及び暗号鍵とセキュリティ処理部19が接続された物理ポートとを、サーチ処理部16を介してIPフローテーブル17に送り、仮登録済みのIPフローエントリの正式登録を行う(ステップ702)。

【0056】パケット処理部14は、当該IPフローに属するパケットに関してサーチ処理部16によるIPフローテーブル17の検索を行った際に、暗号化方式が指定されていること及びIP宛先アドレスが自装置宛であることからIPsec復号化対象パケットであると判断する。そして、当該パケットに対してIPフローテーブル17で指定された暗号化方式等のセキュリティ情報を付加した後、指定された転送先であるセキュリティ処理部19へ転送する(ステップ703)。

【0057】セキュリティ処理部19は、受け取ったパケットからセキュリティ情報を分離し、得られた情報に従って当該パケットをIPsec復号化処理し、カプセル化されたパケットを分離した後、再びパケット処理部14へ転送する(ステップ704)。

【0058】パケット処理部14は、セキュリティ処理部19から受け取ったパケットを、外部のネットワークインタフェースから入力されたパケットと特に区別せず、通常のパケットの様に扱ってIPフローテーブル17の検索を実行する(ステップ705)。この際、パケットはオリジナルのIP宛先アドレスとIP発信元アドレスを持つパケットに復号化されているため、パケット処理部14は新しいIPフローとしてIPフローテーブル17へ仮登録する。

【0059】この後、マイクロプロセッサ11がルーティング処理を行い、処理結果をIPフローテーブル17へ送ってIPフローエントリの正式登録を行う(ステップ706)。ここで、当該パケットは、自装置のサブネットワーク内のホスト宛であると判定されるため、セキュリティ処理は実行されない。

【0060】以上の処理を経た復号化処理済みのパケットは、これ以降、通常のパケット同様に処理される(図3、ステップ313~315、ステップ307~309参照)。また、これ以降、当該復号化対象のパケットと

同一のサーチキー(IP発信元アドレス及びIP宛先アドレス)を有するパケットを受信した場合は、対応するIPフローがIPフローテーブル17に登録されているため、当該登録されているセキュリティ情報を用いて復号化処理を行うことが可能である。したがって、通常のパケットに対するルーティング処理の省略と同様に、マイクロプロセッサ11がセキュリティ情報を取得する処理を行うことなく、パケットがパケット処理部14からセキュリティ処理部19へ送られ、自律的に復号化処理を実行できることとなる。

【0061】以上好ましい実施形態をあげて本発明を説明したが、本発明は必ずしも上記実施形態に限定されるものではない。

【0062】例えば、上記の実施形態では、IPsecの暗号化対象パケットに関して、セキュリティ処理部19によりセキュリティ処理を行った後、当該パケットをパケット処理部14へ戻し、パケット処理部14において通常のパケットと同様に扱うことにより、当該パケットを下位レイヤ処理部20へ転送しているが、このような処理に替えて、以下に示す処理を行っても良い。すなわち、パケット処理部14が、IPパケットのカプセル化、MACヘッダの付加とセキュリティ情報を付加した後、セキュリティ処理部19へと転送する際に、最終的な出力物理ポートの情報も付加して送出する。セキュリティ処理部19は、パケットと共に受信した出力物理ポート情報やMACヘッダを保存しておき、パケットをIPsec暗号化処理した後、パケット処理部14を経由せずに、最終出力物理ポートと接続された下位レイヤ処理部20へ直接転送する。

【0063】以上のような動作を行うためには、ソフトウェア制御によるマイクロプロセッサ11の処理において、通常ルーティング処理と共にカプセル化するIPパケットのIP宛先アドレスに基づくルーティング処理も同時に実行し、その結果をIPフローテーブル17に登録するように変更すれば良い。さらにパケット処理部14とセキュリティ処理部19による処理も、上記動作に併せて追加すれば簡単に実現できる。

【0064】以上のような動作変更を行うことによって、IPsecの暗号化対象パケットに対する図6に示した処理と比較して、さらなるスループットの向上を図ることができる。

【0065】また、上記実施形態では、マイクロプロセッサ11が新しいIPフローに属するパケットのルーティング処理を行う際に、当該パケットのヘッダ部分をパケットメモリ15の結果処理待ちキューからメインメモリ12へコピーしていたが、このような処理に替えて、ヘッダ部分を示すパケットメモリ15のアドレスポインタを受け取って処理を行うことも可能である。すなわち、パケット自体はパケットメモリ15に置かれたままであり、マイクロプロセッサ11は、当該パケットのヘ



ッダ部分を、プロセッサバス13及びパケット処理部14を介して直接読み出す。

【0066】以上のような動作変更を行うことによって、パケットデータの転送回数が最小限に抑えられ、処理の高速化が期待できる。

【0067】さらに、スイッチファブリック18としてクロスバスイッチを採用しても良い。上記実施形態におけるパケットのデータ転送は、基本的に、パケット処理部14と各下位レイヤ処理部20またはセキュリティ処理部19との間における1対1に限られる。しかし、上述したようにセキュリティ処理部19と各下位レイヤ処理部20との間におけるパケット転送が発生する動作を行う場合は、クロスバスイッチの方がデータの衝突の頻度が少なく、全体のスループット向上が可能となる。

【0068】

【発明の効果】以上説明したように、本発明のパケット交換装置によれば、一度マイクロプロセッサによりルーティング処理が実行されたパケットと同一のIP発信元アドレス及びIP宛先アドレスを有するパケットに関しては、マイクロプロセッサを用いたソフトウェア制御によるルーティング処理を行うことなくパケット交換処理を実行することができる。そのため、IPパケットの転送処理の高速化を図ることができるという効果がある。

【0069】また、セキュリティのためのパケットデータの暗号化及び復号化処理を、マイクロプロセッサを用いることなく、ハードウェアにて機械的に実行することにより、セキュリティ処理の高速化を図ることができるという効果がある。

【0070】また、IPフローテーブルを用いてマイクロプロセッサのルーティング処理を行わないパケット転送を実現する構成と、セキュリティ処理を実行するハードウェアとを組み合わせることにより、従来のパケット交換装置と比較して、ネットワークレイヤでのセキュリティ処理を伴うパケット交換を、非常に高速に行うことができる。

【0071】さらに、セキュリティ処理を行うハードウェアをスイッチファブリックの一構成ユニットとすることにより、セキュリティ処理の独立性を高めることができる。これにより、パケット交換装置へのセキュリティ

処理機能の追加や、暗号方式の変更及び追加が容易となるため、パケット交換装置における装置構成の柔軟性及び拡張性の向上を図ることができる。

【図面の簡単な説明】

【図1】 本発明の一実施形態によるパケット交換装置の構成を示すブロック図である。

【図2】 本実施形態におけるIPフローテーブルの例を示す図である。

【図3】 本実施形態におけるパケット処理の主要な流れを示すフローチャートである。

【図4】 本実施形態におけるマイクロプロセッサのルーティング処理の流れを示すフローチャートである。

【図5】 本実施形態におけるセキュリティ処理を伴うパケット処理の流れを示すフローチャートであり、マイクロプロセッサがパケットの種類を認識するまでの動作を示す図である。

【図6】 本実施形態におけるセキュリティ処理を伴うパケット処理の流れを示すフローチャートであり、IPsec暗号化対象パケットに対する処理を示す図である。

【図7】 本実施形態におけるセキュリティ処理を伴うパケット処理の流れを示すフローチャートであり、IPsec復号化対象パケットに対する処理を示す図である。

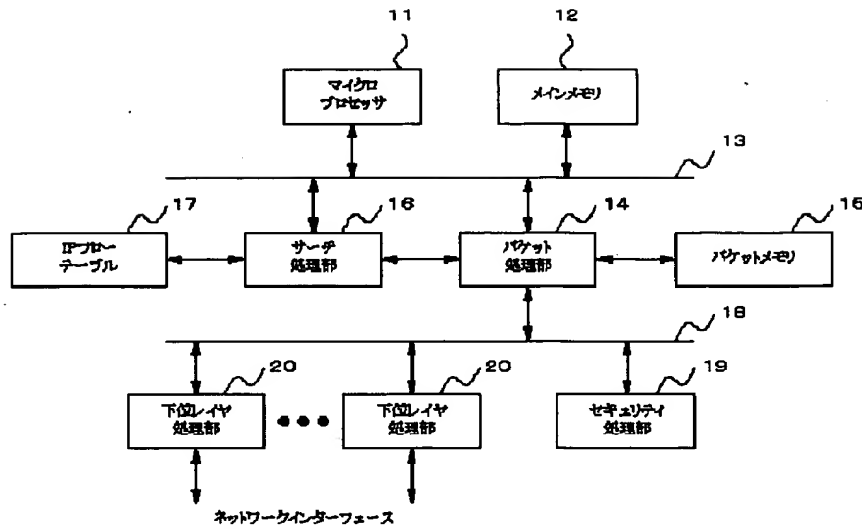
【図8】 IPsecトンネルモードによって処理されたIPパケットの構成を示す図である。

【図9】 従来のパケット交換装置の構成を示すブロック図である。

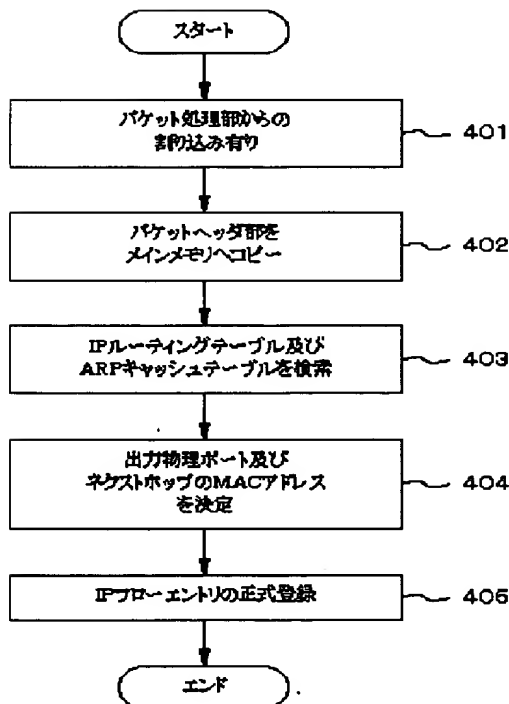
【符号の説明】

- |    |            |
|----|------------|
| 11 | マイクロプロセッサ  |
| 12 | メインメモリ     |
| 13 | プロセッサバス    |
| 14 | パケット処理部    |
| 15 | パケットメモリ    |
| 16 | サーチ処理部     |
| 17 | IPフローテーブル  |
| 18 | スイッチファブリック |
| 19 | セキュリティ処理部  |
| 20 | 下位レイヤ処理部   |

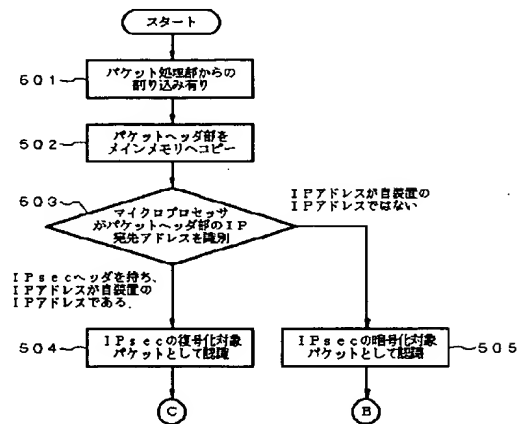
【図1】



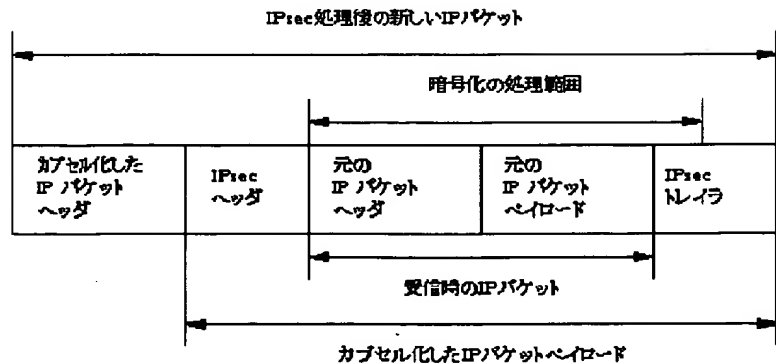
【図4】



【図5】



【図8】



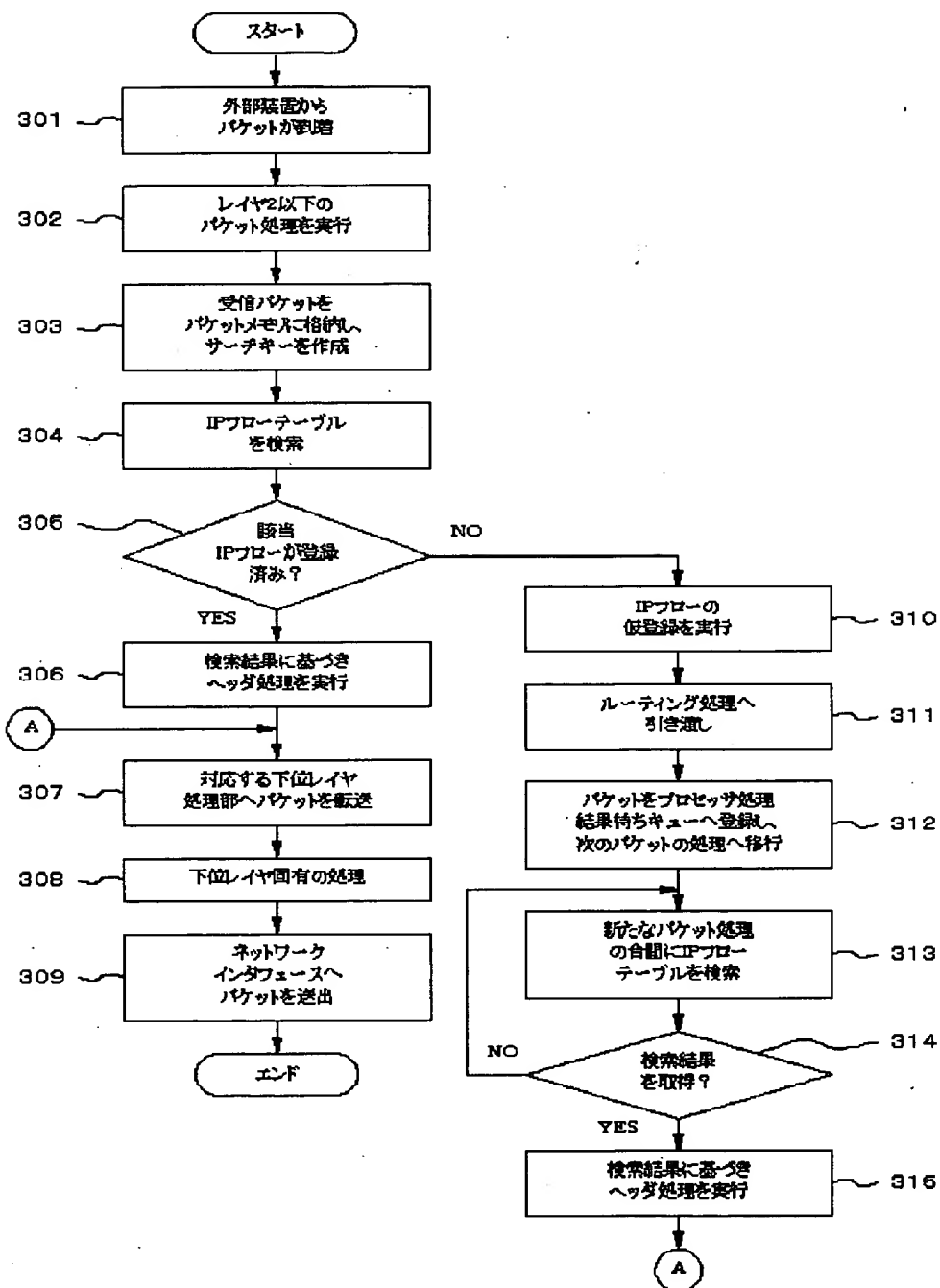
セキユリテイ情報

結果

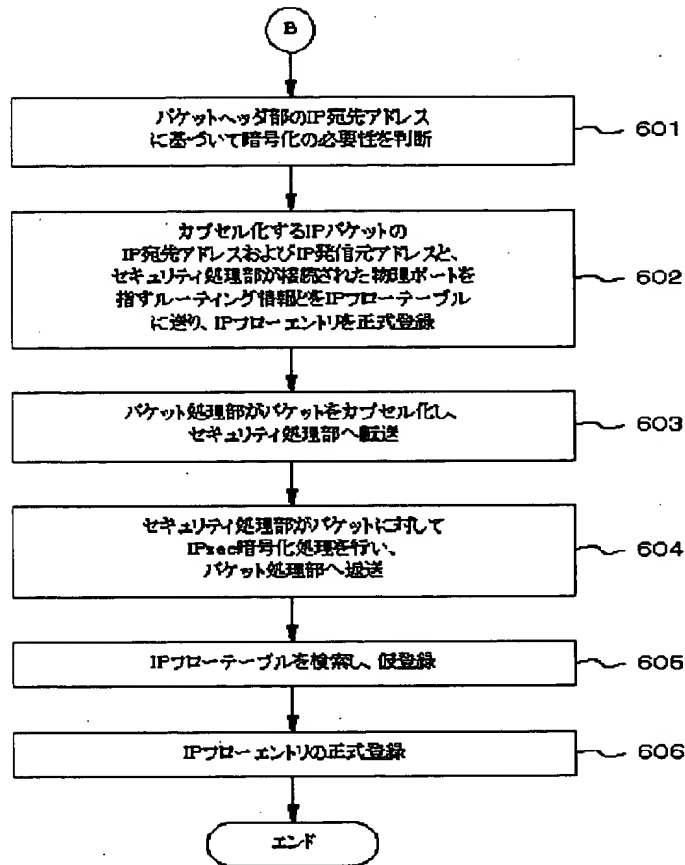
一、

[illegible]

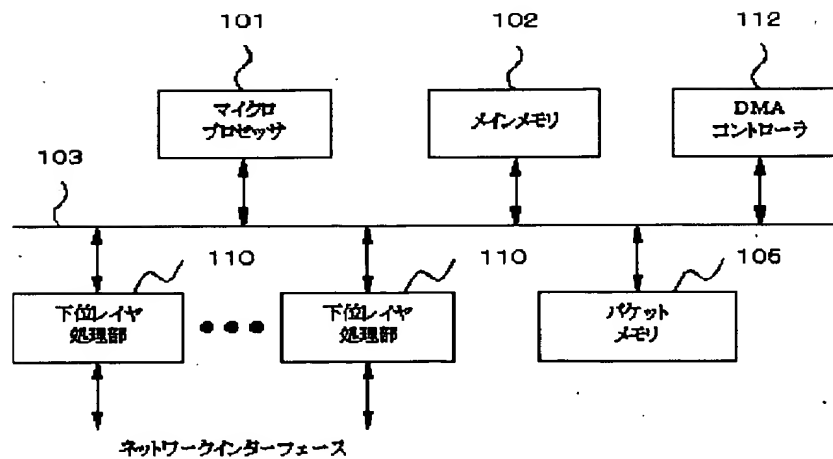
【図3】



【図6】



【図9】



【図7】

